Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, August 23, 2022Randomized and Changing MAC addresses (RCM) |
| Date: 2022-8-23 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Peter Yee | NSA-CSD | Mountain View, CA |  | peter@akayla.com |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11bh telecon meeting of August 23, 2022.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting August 23, 2022 9:30 a.m. to 11:30 a.m. ET**

**Chair: Mark Hamilton (Ruckus/CommScope)**

**Vice Chair: Peter Yee (NSA-CSD/AKAYLA)**

**Vice Chair: Stephen Orr (Cisco)**

**Secretary: Peter Yee**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by the Chair at 9:33 a.m. EDT.**

Agenda slide deck [11-22/1374r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1374-00-00bh-agenda-tgbh-2022-aug-23.pptx)

1. **Policies and procedures were presented by the chair. (Slides 4 to 14)**

There were no Patent declarations.

Copyright policy slides were presented (Slides 10 and 11)

1. **Agenda:**
* **Organization topics (see Backup slides)**
	+ July to Sept teleconferences: Tuesdays, 9:30-11:30 am ET (this time slot)
	+ Timeline reminder (slide 20)
* **Issues Tracking:** [11-21/0332r37](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Reminder: Motions next week: 11-22/0651r2 (motions #9-11, on slides 15-17)**
	+ Discussion: Ready for motion on “Persistent Opaque Identifier”, or alternative suggestion?
* **Results of Comment Collection on D0.2: 11-22/0973r8**
	+ Continue discussion on resolutions of ones that are not on topics:
		- Opt-in, Pre/un-assoc, Non-AP STA-generated ID
	+ 11-22/1069r1 – Resolution of a few comments (Dan Harkins)
	+ 11-22/1078r0 – Device ID indication (Jouni Malinen)
	+ 11-22/1218r3 – Device ID synchronization and control (Kurt Lumbatis)
	+ 11-22/1329r1 – CID resolutions for 12.2.11 (Kurt Lumbatis)
	+ Walk-through CIDs
* **Contributions (slide 16)**
* **WBA liaison response**

Any comments on the proposed agenda? [None]

Any objections to agenda? [None]

With the addition of one more presentation by Kurt Lumbatis (ARRIS/CommScope) to the lineup, the agenda ([11-22/1345r01](https://mentor.ieee.org/802.11/dcn/22/11-22-1345-01-00bh-agenda-tgbh-2022-aug-16.pptx)) was accepted unanimously. There is an understanding that Dan Harkins’ (HPE) and Jouni Malinen’s (Qualcomm) presentations will not be given as neither was able to make the teleconference.

1. **Discussion of Motion #10 on the term “Presistent Opaque Identifier”. Motions will be run next week.**

C- There’s some idea that an identifier is in different states – encrypted and unencrypted. It’s a device ID when unencrypted, but when encrypted it’s an opaque identifier. These wholesale replacements would be a mistake. There are places where persistent opaque identifier makes sense. I’m not sure this is the direction we should go in.

C- When we say opaque, it’s opaque to whom and in what context? It’s opaque over the air? Or to the endpoint? Or to higher layers? Thoughts? Persistent was supposed to indicate that it lasts across MAC address changes and associations back to the same network over time. It’s the underlying ID that’s persistent, not the thing that is sent over the air. Perhaps we aren’t ready for this motion until Antonio de la Oliva can join the conversation.

C- We should use POI everywhere. It’s useful to be able to find everywhere in the spec (over 6,000 pages) to find the term with a search.

C- The editor will take care of the expansion as necessary.

C- I don’t like the term. It sounds wrong. You can’t have an Annex Z that talks about opaque identifier and then use it everywhere else in the document. Also, POI has another well-known meaning - place of interest on GPS. I think NGID, as originally proposed, is fine.

C- NGID may not be appropriate because we haven’t settled on where the ID is generated in all cases. That may be one reason to wait. We aren’t quite settled on this. Antonio may need to bring a presentation when he’s back. I see in the chat the term “persistent private identifier”. Let’s wait for Antonio’s return.

1. **Resolution of a Few Comments**

Dan Harkins spoke about 11-22/1069r00.

CID 21- what is the meaning of “foil traffic analysis” in the context of the sentence? Given a definition for “traffic analysis” from a popular search engine, the meaning of “foil” should be clear. Therefore, the comment should be rejected.

C- There are probably other definitions out there of what traffic analysis is. Have you considered adding the one you are using to the document so that it’s clear?

Q- In the definition of terms section?

A- Probably.

C- I can generate a new version of the resolutions with a revised resolution for this comment.

Q- Is the term traffic analysis used elsewhere in IEEE 802.11?

A- I believe so, although that doesn’t mean it’s understood.

C- It might be useful to check on that.

C- That would require us to make sure the definitions don’t clash. I’ll check on that.

C- Let’s not use the term “foil” as that’s a bit non-obvious for non-English speakers. Let’s use something like “prevent”.

C- [Quote from section 4.5 on traffic analysis.]

C- That’s good background and let’s make sure we’re aligned.

Q- So, should we add something to 3.2, or just change “foil” to “mitigate” or “prevent”?

A- Seems all right.

Q- Does anyone feel we do need a definition given the term already is used in the baseline?

A- Typically, if a term is used in more than one location, then we end up adding a definition. If used in only one location, we define it inline. But I’m not sure we are using the term in the same manner as the existing usage.

A- It is the same usage. It’s looking at a set of messages to infer something, even when the content can’t be read. This is why MAC addresses, that can be read, are changed.

C- The proposed resolution would be to change “foil” to “mitigate”.

Q- Do we now need a formal definition?

Q- That’s up to the group. Do you have an opinion?

A- I think we should define it given that it appears in multiple, disparate places.

C- I’ll note that the quote refers to “this sort of traffic analysis”. We should check to make sure there isn’t some other kind implied elsewhere in the document. We should also check the IEEE dictionary to see if we are aligned.

C- This quote probably came in from IEEE 802.11aq, so I thought it would be familiar.

C- I’ll make a revision of the comment resolutions with a new resolution for CID 21.

For CID 22, I propose rejecting it. The size of the identifier isn’t part of the overhead. The overhead is what protects the identifier. Annex Z allows for variable size tweaks, but it does define how to calculate the overhead size.

C- The comment is quoting the text. The commenter is saying that for an 8-octet tweak, the overhead is 25 octets plus the padding. The commenter might be saying that the padding size isn’t known ahead of time.

C- The padding should be different each time, so the overhead varies.

Q- Why can’t you say 25 octets plus the padding?

A- It differs each time.

C- The comment asks if blob (ID) is fixed or variable.

Q- Is it clear in the text?

A- We don’t describe how to construct the device ID itself. It’s generated by the network. We don’t say it has a fixed value. I’m not sure that informative Annex Z is the right place to say that.

C- We have some proposals that have it as a MAC address. It might make sense to say in the annex that there’s no assumption about the length of the blob.

C- I can do that.

Q- Does the blob have a fixed or variable value. The ID blob is the number of bits in the 4-way handshake KDE?

A- No. That includes the blob and the padding. To foil traffic analysis, the padding needs to differ each time. That’s the whole idea. It can’t be fixed. Are you referring to the blob or the whole thing?

A- The AP generates a device ID and generates a blob, which is placed in the KDE, right?

Q- Given that the padding is going to be a different length each time, how do we calculate a fixed value for what goes in the KDE?

A- It’s how many octets you can put in the KDE. It says make the length of the padding every time. The encrypted length will be different every time. I’m not understanding the confusion.

C- If we look at the sentence that says an 8-octet tweak it’s a 25-octets. I think the confusion is that the sentence makes it look like a fixed length.

C- There’s no length indication. So how does the STA receive the ID blob? If you look at the device ID element that has a length indication. But in the EAPOL frame, in the KDE part, there’s no length indication.

C- That’s solved in the 4-way handshake text, not in Annex Z. This is not the place to discuss how to parse the 4-way handshake. I’m happy to assign the comment to someone else.

C- If there’s a problem in the baseline if we don’t define if it’s fixed length or variable.

C- Annex Z is informative. This non-problem shouldn’t impinge on the baseline.

Q- I’ve seen comments to delete that sentence. What do you think?

A- Okay.

Q- Does the annex say that the part that gets encrypted is fixed length or variable?

A- The commenter thinks it’s the encryption output length being discussed. For the network-generated ID, the length is probably fixed. The input has a fixed length, but the output does not. That’s the whole point.

C- Instead of deleting the sentence on 25 octets, it would be clearer to add “plus padding” to the sentence. It’s just an example of how to do the summation.

C- I don’t think the sentence is necessary, although I wouldn’t object to adding “plus padding”, but I don’t think basic math is needed here.

C- The document says that the device KDE is the ID blob. That’s the confusion.

Q- Where does it say ID blob in Annex Z? If you think there’s a problem with the 4-way handshake, file another comment.

A- Annex Z doesn’t say blob. It’s confusing with all the definitions.

C- That’s going to be resolved by a previous discussion, not by CID 22.

Q- How do you feel about adding “plus padding” to the sentence?

A- I think removing the sentence is fine – there’s no need to do basic math.

Q- How does the group feel about deleting the sentence? I also agree we need to align our terminology.

C- No objection to deleting it seen.

CID 23. I suggest the how is irrelevant and inappropriate for this annex. We don’t talk about how APs share information, except in IEEE 802.11f, which has been removed. Basically, how the key is managed is unnecessary and out of scope.

C- We sometimes put a throwaway note about this being outside of the scope of the standard.

Q- Thoughts?

A- I could do that, although I favor rejecting it. There are plenty of places in the standard where we don’t answer these kinds of questions. I’d rather follow the convention.

C- I support the rejection. Adding a note in the annex, which is non-normative, isn’t necessary where it might be in the main body text.

Q- Any problem with rejecting this comment with the given rationale?

A- None seen.

CID 34. I propose accepting this.

CID 54. The comment is correct but removing “without modification” makes the sentence odd. Rewriting the sentence makes it clearer.

C- I thought we already had a sentence about the most recently received value. It’s awkwardly worded. I think we fixed it somewhere else.

C- I have something in one of my previous resolutions. I don’t have the exact wording at hand.

C- Okay, then in the next revision of the resolutions, I’ll mark it as revised as a duplicate [and covered by CID 3].

C- I think that two people are making the same point. I think the best practice is to give the changes and optionally point at CID 3.

C- That makes a problem for the editor, having two versions of the comment resolved.

C- Why don’t we say “revised, as in 1082r04”. Both resolutions will point to the same resolution.

C- If both refer to the same document, I’ll make the changes in the document and that will count against both CIDs.

C- The reason that we require a complete resolution for each comment is because when we go to SA ballot, the numbering or document references are hard for SA balloters to figure things out. The best thing is either to have a single document with the proposed change, or to say in the duplicated resolution that this is the same change as another comment.

1. **TG bh: Background, Use Cases, PAR, Privacy etc.**

This presentation is a reaction to the “pre-association use cases” discussion. It gives background on the RCM TIG agreeing that things like band steering and other pre-association use cases should be addressed. Maybe calling all of these things “pre-association” may be the wrong term, but they were dealt with in the TIG report. The TGbh PAR also talks about the existing services. It wasn’t contentious and passed unanimously. Given that background, the scope could be seen as “things that RCM broke”. The market seems to have treated that as “use the same address for the same BSS”. Thus, leading up to the approval of TGbh, it was fully understood that pre-association was in scope.

Now, some task group members have expressed the opinion that pre-association is not needed. The proposed pre-association schemes do meet all the use cases. These can be called the pre-schemes. Do we need them in addition to device ID? Should we have alternative schemes in IEEE 802.11bh or just stick to one. Going back to 2014, WNG has seen privacy concerns addressed, for example in Paul Lambert’s (Marvell) presentation. IEEE 802.11bh must not violate the passive tracking protection. RCM prevents passive monitoring of probes, which is the same as what the pre-schemes try to do. The pre-schemes allow a STA returning to the same AP to prevent listeners from discovering this. The pre-schemes help with scenario 1 (slide 19), but not completely. Just the fact that a STA tries to associate with a specific AP is giving away that someone who “knows” that SSID is trying to associate with it. Fixing that problem is probably an IEEE 802.11bi issue. In scenario 2, with a STA using a one-time address, a listener can’t even tell it is a returning STA. My argument is that the pre-schemes are not worse from a privacy perspective than RCM and do solve a problem that the WBA expects us to solve. TGbh should answer the question if there are use cases that are not covered by Device ID. And should we offer another scheme to cover them?

Steering has been done with BSS transition management (BTM) and Neighbor Report. BTM is post association. Neighbor Report ANQP exists, but only for a 6 GHz BSS. A STA sends a Query ID for Neighbor Report (apparently only for 6 GHz APs). That might work for other situations. Then the question is if the STA should know who it is talking to.

In use case 4.1 (pre-association steering), there are several questions that arise. It’s not clear how pre-association steering worked prior to RCM and how RCM broke it.

In use case 4.2 (home control), these just work off a list of MAC addresses. RCMs defeat that. Device ID schemes work here, but only post association. Pre-schemes would require that the newly assigned address be added to the allow list, but that’s not hard.

Use cases 4.9 and 4.10 (steering), it would be nice to deal with this pre-association from a latency perspective.

Remember, IEEE 802.11bh is optional and opt-in. Thus, allowing the AP/BSS to select what it wants to support and use is the right choice. This choice will be up to a higher layer application. Thus, if we don’t support pre-association, the task group should consider disbanding or amending its PAR.

C- I’ll note that this is timely with one of the motions next week.

C- It’s not clear to me that the PAR requires pre-association schemes or prevents them. I don’t think we’ll support every existing service. We’ve already decided that some are misguided or not to be maintained.

C- My point is that those use cases were covered in the TIG report and were well understood to be worth addressing.

C- You mentioned the Neighbor Report ANQP and said it wasn’t clear where it’s required. Neighbor Report has been in the spec for quite a while, but it is not required except for certain 6 GHz discovery use cases. The Wi-Fi Alliance certification on agile multiband does require Neighbor Report use for pre-association discovery of the “best” or preferred AP. This is required in IEEE 802.11ax certification. It’s not a hard requirement in IEEE 802.11.

Q- Does the agile multiband stuff work with RCM?

A- That’s a question for AP vendors. It’s a challenge. Lots of device are pseudo-static with their RCM addresses while they are probing, but it’s hit-and-miss in terms of device behaviors.

C- That might make a nice presentation as support for a pre-scheme.

C- I think I did something like that on the reflector.

Q- People who are arguing against pre-schemes seem to imply that the device ID only exists in the 4-way handshake, but is that an accurate observation? Does the ID only exist in the protected KDE in the 4-way handshake? I was under the impression that the ID that was exchanged in the 4-way handshake could then be used in the pre-schemes or outside of the 4-way handshakes.

C- My question is unrelated to that. I agree that we should not interpret the PAR too much. I see discussion of cross-ESS use cases because some people use that in existing service. Looking at section 5.2.b of the PAR, does existing service mean cross-ESS as well? I don’t agree that we must change the PAR even we don’t cover cross-ESS. Don’t read too much into the PAR.

Q- Could you identify a cross-ESS use case that has been discussed?

A- It was in an email (on the reflector). Maybe I misunderstood. Not talking about cross-ESS is good.

C- If we come up with a solution that someone then says that it doesn’t look like you fixed my problem, it’s not a good look. The PAR is extremely important.

C- There have been several presentations so that the next time the STA comes back in it can be identified pre-association. Graham has made such proposals. I do agree that slide 5, use case 3.1 covers the pre-association need. There exist mechanisms that would address that use case.

C- The arguments over the PAR reflect the arguments we had at the formation of the group over boundaries. Some believe pre-association use cases are critical. Others do not. Graham has outlined why he believes that there are techniques that would help people to retain services that worked pre-RCM. The question is whether these use cases are important enough. I believe they are.

C- The group should think a bit more about pre-association probing.

**Meeting adjoined at 11:30 a.m. EDT.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 8/23 | Ansley, Carol | Cox |
| TGbh | 8/23 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 8/23 | Harkins, Dan | HPE |
| TGbh | 8/23 | Henry, Jerome | Cisco |
| TGbh | 8/23 | Huang, Po-Kai | Intel |
| TGbh | 8/23 | Kneckt, Jarkko | Apple |
| TGbh | 8/23 | Levy, Joseph | InterDigital |
| TGbh | 8/23 | Lumbatis, Kurt | ARRIS/CommScope, Inc. |
| TGbh | 8/23 | Mutgan, Okan | Nokia |
| TGbh | 8/23 | Orr, Stephen | Cisco Systems, Inc. |
| TGbh | 8/23 | Petrick, Al | InterDigital |
| TGbh | 8/23 | Rison, Mark | Samsung |
| TGbh | 8/23 | -Sam, Harvey | Broadcom Corporation |
| TGbh | 8/23 | Sevin, Julien | Canon |
| TGbh | 8/23 | Smith, Graham | SRT Wireless |
| TGbh | 8/23 | Smith, Luther | CableLabs |
| TGbh | 8/23 | Stanley, Dorothy | HPE |
| TGbh | 8/23 | Sun, Bo | ZTE |
| TGbh | 8/23 | Thakore, Darshak | CableLabs |
| TGbh | 8/23 | Thakur, Sidharth | Apple |
| TGbh | 8/23 | Yang, Jay | Nokia |
| TGbh | 8/23 | Yee, Peter | NSA-CSD |